Partial Listing

US005659616A

# United States Patent [19]

Sudia

[11] Patent Number: 5,659,616

[45] Date of Patent: Aug. 19, 1997

[54] **METHOD FOR SECURELY USING DIGITAL SIGNATURES IN A COMMERCIAL CRYPTOGRAPHIC SYSTEM**

[75] Inventor: **Frank Wells Sudia**, New York, N.Y.

[73] Assignee: **Certco, LLC**, New York, N.Y.

[21] Appl. No.: **682,871**

[22] Filed: **Jul. 16, 1996**

**Related U.S. Application Data**

[63] Continuation of Ser. No. 277,438, Jul. 19, 1994, abandoned.

[51] **Int. Cl.**[6] ..... **H04K 1/00**

[52] **U.S. Cl.** ..... **380/23**; 380/25; 380/30

[58] **Field of Search** ..... 380/23, 25, 24, 380/4, 3, 49, 29, 30

[56] **References Cited**

U.S. PATENT DOCUMENTS

| | | | |
|---|---|---|---|
| 4,625,076 | 11/1986 | Okamoto et al. | 380/23 |
| 4,981,370 | 1/1991 | Dziewit et al. | 380/25 |
| 5,005,200 | 4/1991 | Fischer | 380/30 |
| 5,031,214 | 7/1991 | Dziewit et al. | 380/23 |
| 5,157,726 | 10/1992 | Merkle et al. | 380/23 |
| 5,163,091 | 11/1992 | Graziano et al. | 380/25 |
| 5,191,613 | 3/1993 | Graziano et al. | 380/215 |
| 5,214,702 | 5/1993 | Fischer | 380/30 |

OTHER PUBLICATIONS

ANSI X9.30–199x (Working Draft) Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry: Part 3: Certificate Management for DSA, Jun. 1, 1994, pp. i–86.

Secure Data Network System, Access Control Specification, Access Control Information Specification (ACIS) Addendum 1 (SDN.802/1), Jul. 25, 198 pp. ii–85.

Secure Data Network System, Access Control Specification, SDN.802, Rev. 1.0 Jul. 25, 1989, pp. 1.43.

Secure Data Network System; Access Control Concept Document (Revision 1.3), SDN.801, Jul. 26, 1989, pp. 1–18.

European Computer Manufacturers Association, Standard ECMA–138 Security in Open Systems —Data Elements and Service Definitions, Dec. 1989, pp. i–81.

Addison Fischer, Workflow. 2000–Electronic Document Authorization in Practice, Fischer International Systems Corporation, Copyright 1992, 7 pages.

Richard Ankney, Certificate Management for the Financial Services Industry, Aba/Scitech/Notaization and Nonrepudiation WG. Mtg. of Jul. 1, 1993.

ANSI X9.30 (Working Draft) Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry: Part 3: Certificate Management for DSA, Mar. 29, 1993, pp. i–71.

ANSI X9.30–199x (Working Draft) Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry: Part 3: Certificate Management of DSA, Sep. 27, 1993, p. i–87.

Rich Ankney, et al. Enhanced Management Controls Using Attribute Certificates, ASC X9 Project Proposal No. X9F–1–3, Nov. 10, 1993, 13 pages.

(List continued on next page.)

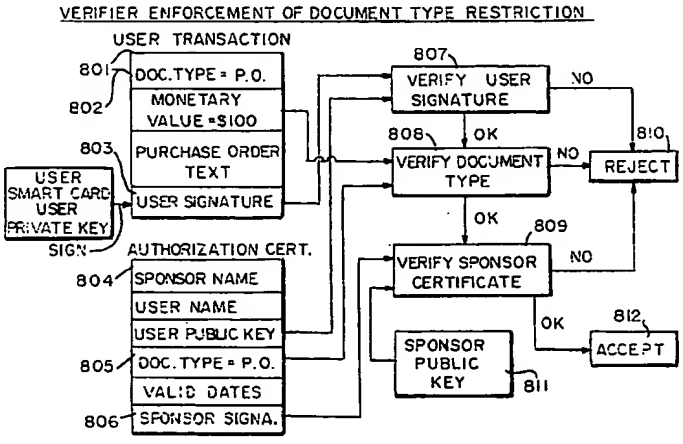
*Primary Examiner*—David C. Cain

*Attorney, Agent, or Firm*—Cushman, Darby & Cushman IP Group of Pillsbury Madison & Sutro LLP

[57] **ABSTRACT**

A system for securely using digital signatures in a commercial cryptographic system that allows industry-wide security policy and authorization information to be encoded into the signatures and certificates by employing attribute certificates to enforce policy and authorization requirements. In addition to value limits, cosignature requirements and document type restrictions that can be placed on transactions, an organization can enforce with respect to any transaction geographical and temporal controls, age-of-signature limitations, preapproved counterparty limitations and confirm-to requirements by using attribute certificates for the transacting user. Restrictions on distribution of certificates can be set using attribute certificates. Certificates can be used also to ensure key confinement and non-decryption requirements of smartcards in this system.

**37 Claims, 15 Drawing Sheets**



US-PAT-NO: 5659616

DOCUMENT-IDENTIFIER: US 5659616 A

TITLE: Method for securely using digital signatures in a commercial cryptographic system

---------- KWIC ---------

Detailed Description Text - DETX (44):

The attribute values of delegation controls can limit the types and value ranges of authorizations that a CA may specify when issuing an attribute certificate. They can also serve to limit the scope and depth to which a user may delegate his signing authority to others. For example, a root CA might limit an organizational CA to issuing authorizations only to allow its end users to sign documents whose document types fall into a range of documents related to state **tax** administration. Or a CA might grant some authority to a user with the provision that it can be delegated only to another person with the rank of assistant treasurer or higher, for a time not to exceed thirty days, and without the right to further subdelegate.

Detailed Description Text - DETX (48):

A set of basic policies must be defined for use throughout the financial services industry and other industries in order to provide a well-defined, predictable level of service for the verification process. These policies would be agreed to on a multilateral basis by every participating firm and could stipulate that certain of the restrictions and authorizations discussed in this section would always be deemed to be in effect unless expressly provided otherwise. One of the more important elements of these industry agreements would be the definition and coding of document types. This must be done on a per-industry basis, since the rules will obviously be much different, for instance, for customs inspectors, aircraft inspectors, auditors, **tax** officials, etc.

Current US Cross Reference Classification - CCXR (4):

**713/156**